<u>REMARKS</u>

This application has been reviewed in light of the final Office Action dated May 3, 2006. Claims 1-4, 6-10, 12, 13, and 15-18 are presented for examination. Claims 1, 4, 6, and 12 have been amended to define more clearly what Applicants regard as their invention. Claims 17 and 18 have been added to provide Applicants with a more complete scope of protection. Claims 1, 4, 9, 12, 17, and 18 are in independent form. Favorable reconsideration is requested.

Initially, the Office action asserts, incorrectly, that the Information Disclosure Statement filed May 21, 2001, is improper in that it did not include a form PTO-1449 (or equivalent) listing the cited document. Since the only document cited was a copending U.S. patent application, a form PTO-1449 is not required. See MPEP Section 609. Accordingly, consideration of the Information Disclosure Statement is respectfully requested.

Claims 1-4, 6-10, 12, 13, 15, and 16 were rejected under 35 U.S.C. § 103(a) as being obvious from U.S. Patent No. 5,633,932 (*Davis*) in view of U.S. Patent 5,191,611 (*Lang*).

An aspect of the present invention to which Claim 1 relates is a method for secure remote printing from an originating device to a printer using a physical security key embodying a private key.

Independent Claim 1 is directed to a method of conducting, in relation to a print job, a printing process between an originating device and a printer, the method including the steps of initiating the printing process at the originating device for outputting the print job from the printer; encrypting, at the originating device, the print job with a public key corresponding to a private key. The method further includes the steps of suspending the printing process prior to outputting the print job from the printer; connecting a physical security key, which embodies the

- 11 -

private key corresponding to the public key, to the printer; decrypting, at the printer, the print job with the private key embodied by the physical security key connected to the printer; and enabling, after decrypting the print job with the private key, the suspended printing process to output the print job from the printer.

Among notable features of the method of Claim 1 are that after a physical security key, which embodies a private key corresponding to a public key, is connected to a printer, the method decrypts, at the printer, a print job with the private key embodied by the physical security key connected to the printer, and enables, after decrypting the print job with the private key, a suspended printing process to output the print job from the printer.

Davis, as understood by Applicants, relates to a system and method for preventing a printing of a document until a printing node authenticates the intended recipient. In *Davis*, a printing node simply matches the public key of the token, which may be a PCMCIA identifier card or a smart card that can be inserted into the printing node, to a public key previously received in a header of a print job. See col. 5, lines 52-60, for example.

In contradistinction to the method of Claim 1, in which after a physical security key embodying a private key is connected to a printer, a print job is decrypted using the private key and a suspended printing process is enabled to output the print job from the printer, in *Davis*, the printing node merely matches a public key of a token to a public key received in a header of a received document.

Applicants submit that nothing has been found in *Davis* that would disclose or suggest that after a physical security key embodying a private key is connected to a printer, a print job is decrypted using the private key and a suspended printing process is enabled to output

the print job from the printer, as set forth in Claim 1.

Lang, as understood by Applicants, relates to a method and apparatus for protecting material on storage media and for transferring material on storage media to various recipients.

Applicants submit that nothing has been found in *Lang* that would disclose or suggest that after a physical security key embodying a private key is connected to a printer, a print job is decrypted using the private key and a suspended printing process is enabled to output the print job from the printer, as set forth in Claim 1.

Accordingly, Claim 1 is seen to be clearly allowable over *Davis* and *Lang*, whether considered separately or in any permissible combination (if any).

Independent Claims 4, 9, 12, 17, and 18 each recite features similar in many relevant respects to those discussed above with respect to Claim 1, and are also believed to be patentable over *Davis* and *Lang* for at least the reasons discussed above.
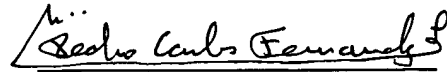
A review of the other art of record has failed to reveal anything which, in Applicants' opinion, would remedy the deficiencies of the art discussed above, as references against the claims herein. Those claims are therefore believed patentable over the art of record.

The other claims in this application depend from one or another of the independent claims discussed above and, therefore, are submitted to be patentable for at least the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, individual consideration or reconsideration, as the case may be, of the patentability of each claim on its own merits is respectfully requested.

In view of the foregoing amendments and remarks, Applicants respectfully request favorable reconsideration and early passage to issue of the present application.

Applicants' undersigned attorney may be reached in our New York Office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address listed below.

Respectfully submitted,

Pedro C. Fernandez
Attorney for Applicants
Registration No.: 41,741

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

NY_MAIN 579077v1